CHAPTER 2

COMMAND SECURITY MANAGEMENT

2-1 COMMANDING OFFICER

1. **Terminology.** **"Command"** is used as a generic term for any organizational entity and may include a base, station, unit, laboratory, installation, facility, center, activity, detachment, squadron, ship, etc. **"Commanding officer"** is used throughout this regulation as a generic term for the head of any DON command and includes commander, commanding general, director, officer in charge, etc.

2. **Responsibility and Authority.** The commanding officer is responsible for the effective management of the ISP within the command. Authority delegated by this regulation to a commanding officer may be further delegated unless specifically prohibited.

3. **Standards.** This regulation establishes baseline standards, but the commanding officer may impose more stringent requirements within the command or upon subordinates if the situation warrants. The commanding officer shall not, however, unilaterally establish requirements that impact on other commands or cleared DoD contractors, or that contradict this regulation or reference (a).

4. **Risk Management.** Commands confront different environments and sets of changing operational requirements. Therefore, each commanding officer shall apply risk management principles to determine how best to attain the required levels of protection. Employing risk management results in command decisions to adopt specific security measures given the relative costs and available resources.

5. **Implementation.** The commanding officer shall designate, in writing, certain security personnel directly involved in program implementation (see paragraphs 2-2 through 2-9). Additionally, the commanding officer shall:

   a. Issue a written command security instruction (see **exhibit 2A**).

   b. Approve an emergency plan which includes provisions for the protection and destruction of classified information in emergency situations (see **exhibit 2B**).

c. Establish and maintain a self-inspection program for the command. This may include security inspections, program reviews, and assist visits to evaluate and assess the effectiveness of the command's ISP (see **exhibit 2C**).

d. Establish an industrial security program when the command engages in classified procurement or when cleared DoD contractors operate within areas under their direct control.

e. Apply risk management, as appropriate, for the safeguarding of classified information, and monitor its effectiveness in the command.

f. Ensure that the security manager and other command personnel receive training as required, and support the command security education program.

g. Inform command personnel that they are expected and encouraged to challenge the classification of information which they believe to be improperly classified and ensure that procedures for challenging and appealing such status are understood.

h. Ensure that the performance rating systems of all DON military and civilian personnel, whose duties significantly involve the creation, handling, or management of classified information, include a critical security element on which to be evaluated.

2-2 SECURITY MANAGER

1. The commanding officer shall designate, in writing, a command security manager. The security manager is responsible for implementing the ISP and shall have direct access to the commanding officer. Some tasks may be assigned to a number of command personnel and may even be assigned to persons senior to the security manager. Nevertheless, the security manager shall remain cognizant of all command information, personnel, and industrial security functions and ensure that the security program is coordinated and inclusive of all requirements in this regulation. The security manager shall:

a. Serve as the principal advisor and representative to the commanding officer in matters pertaining to the classification, safeguarding, transmission, and destruction of classified information.

b. Develop a written command security instruction (see exhibit 2A), to include provisions for safeguarding classified information during military operations or emergency situations.

c. Ensure that personnel in the command who perform security duties are kept abreast of changes in policies and procedures, and provide assistance in problem solving.

d. Formulate, coordinate, and conduct the command security education program.

e. Ensure that threats to security, and other security violations are reported, recorded, and, when necessary, investigated. Ensure that incidents described in chapter 12 of this regulation are immediately referred to the nearest NCIS office.

f. Coordinate the preparation and maintenance of security classification guides under the command's cognizance.

g. Maintain liaison with the command Public Affairs Officer (PAO) to ensure that proposed press releases and information intended for public release are subjected to a security review (see chapter 8).

h. Coordinate with other command officials regarding security measures for the classification, safeguarding, transmission and destruction of classified information.

i. Develop security measures and procedures regarding visitors who require access to classified information.

j. Ensure that classified information is secured and controlled areas are sanitized when a visitor is not authorized access.

k. Implement and interpret, as needed, regulations governing the disclosure of classified information to foreign governments.

l. Ensure compliance with the requirements of this regulation when access to classified information is provided at the command to industry in connection with a classified contract.

m. Ensure that access to classified information is limited to appropriately cleared personnel with a need-to-know per reference (b).

2. The command security manager may be assigned full-time, part-time or as a collateral duty and must be an officer or a civilian employee, GS-11 or above, with sufficient authority and staff to manage the program for the command. The security manager must be a U.S. citizen and have been the subject of a favorably adjudicated Single Scope Background Investigation (SSBI) completed within the previous 5 years.

3. The security manager shall be identified by name on command organizational charts, telephone listings, rosters, or other media. Reference (c) recommends that the security manager report to the commanding officer on functional security matters and to the executive officer for administration of the ISP.

2-3 TOP SECRET CONTROL OFFICER (TSCO)

1. The commanding officer shall designate, in writing, a command TSCO for commands handling Top Secret information. A Top Secret Control Assistant(s) (TSCA(s)) may be assigned as needed (see paragraph 2-4.4). The TSCO reports directly to the security manager or the security manager may serve concurrently as the TSCO. The TSCO shall:

a. Maintain a system of accountability (e.g. registry) to record the receipt, reproduction, transfer, transmission, downgrading, declassification and destruction of command Top Secret information, less SCI and other special types of classified information.

b. Ensure that inventories of Top Secret information are conducted at least once annually, and more frequently when circumstances warrant (see chapter 7, paragraph 7-3). As an exception, repositories, libraries, or activities which store large volumes of classified documents may limit their annual inventory to that which access has been given in the past 12 months, and 10 percent of the remaining inventory.

2. The TSCO must be an officer, senior non-commissioned officer E-7 or above, or a civilian employee, GS-7 or above. The TSCO must be a U.S. citizen and have been the subject of an SSBI completed within the previous 5 years.

2-4 OTHER SECURITY ASSISTANTS

1. **Assistant Security Manager.** In large commands and where circumstances warrant, the commanding officer shall designate, in writing, a command assistant security manager to assist in program implementation and maintenance. The responsibilities

assigned to assistant security managers shall be commensurate with their grade level and experience, understanding that the security manager will provide the guidance, coordination, and oversight necessary to ensure that the program is being administered effectively.

2. A person designated as an assistant security manager must be a U.S. citizen, and either an officer, enlisted person E-6 or above, or civilian employee GS-6 or above. Assistant security managers must have an SSBI if they are designated to issue interim security clearances; otherwise, the investigative and clearance requirements will be determined by the level of access to classified information required.

3. **Security Assistant.** Civilian and military member employees performing administrative functions under the direction of the security manager may be assigned without regard to rate or grade as long as they have the clearance needed for the access required to perform their assigned duties and taskings.

4. **TSCA(s).** The commanding officer shall designate, in writing, a TSCA(s) to assist the TSCO, as needed. Top Secret couriers are not considered to be TSCA(s).

5. A person designated as a TSCA must be a U.S. citizen and either an officer, enlisted person E-5 or above, or civilian employee GS-5 or above. An established Top Secret security clearance eligibility is required.

2-5 SECURITY RELATED COLLATERAL DUTIES

1. **CMS Custodian.** Reference (d) requires that the commanding officer designate, in writing, a CMS custodian and an alternate to manage COMSEC information issued to a CMS account. The CMS custodian is the commanding officer's primary advisor on matters concerning the security and handling of COMSEC information and the associated records and reports.

2. **Naval Warfare Publications (NWP) Custodian.** Reference (e) requires the commanding officer to designate, in writing, an NWP custodian. This assignment is normally a collateral duty. The NWP custodian receipts and accounts for NWPs, ensures completion of Preliminary Inquiries (PIs) and Judge Advocate General Manual (JAGMAN) investigations for loss or compromised publications, and provides procedures for inclusion in the command emergency action plan.

3. **NATO Control Officer.** The commanding officer shall designate, in writing, a command NATO control officer and at least one alternate to ensure that NATO information is correctly controlled and accounted for, and that NATO security procedures are observed. Reference (f) establishes procedures and minimum security standards for the handling and protection of NATO classified information. The CUSR is the main receiving and dispatching element for NATO information in the U.S. Government. The CUSR manages the U.S. Registry System of subregistries and control points to maintain accountability of NATO classified information.

2-6 CONTRACTING OFFICER'S REPRESENTATIVE (COR)

The contracting officer shall designate, in writing, one or more qualified security specialists per Subpart 201.602-2 of reference (g), as CORs, previously called "Contracting Officer's Security Representative." The designation shall be for the purpose of signing the Contract Security Classification Specification (DD 254), and revisions thereto. The COR is responsible to the security manager for coordinating with program managers and procurement officials. The COR shall ensure that the industrial security functions specified in chapter 11 are accomplished when classified information is provided to industry for performance on a classified contract.

2-7 INFORMATION SYSTEMS SECURITY MANAGER (ISSM)

Per reference (h), the commanding officer shall designate, in writing, an ISSM and Information Systems Security Officer(s) (ISSOs), as appropriate. The ISSM serves as the point of contact for all command INFOSEC matters and implements the command's INFOSEC program. ISSOs are designated for each information system and network in the command responsible for implementing and maintaining the command's information system and network security requirements. In some commands, the ISSM and ISSO duties may be performed by the same person.

2-8 SPECIAL SECURITY OFFICER (SSO)

1. Per reference (i), the commanding officer shall designate, in writing, a command SSO and Subordinate Special Security Officer (SSSO), as needed, for any command that is accredited for and authorized to receive, store, and process SCI. The SSO is responsible for the operation (e.g. security, control, use, etc.) of all command Sensitive Compartmented Information Facilities (SCIFs). All SCI matters shall be referred to the SSO. The SSO may be designated as security manager if the grade requirements

for security manager are met; however, the security manager cannot function as an SSO unless designated by the Director, ONI or COMNAVSECGRU.

2. The SSO and the SSSO must be a U.S. citizen and either a commissioned officer or a civilian employee GS-9 or above, and must meet the standards of reference (j).

2-9 SECURITY OFFICER

Per reference (k), the commanding officer shall designate, in writing, a command security officer. This official may serve concurrently as security manager.

2-10 SECURITY SERVICING AGREEMENTS (SSAs)

1. Specified security functions may be performed for other commands via SSAs. Such agreements may be appropriate in situations where security, economy, and efficiency are considerations, including:

a. A command provides security services for another command, or the command provides services for a tenant activity;

b. A command is located on the premises of another government entity and the host command negotiates an agreement for the host to perform security functions;

c. A senior in the chain of command performs or delegates certain security functions of one or more subordinate commands;

d. A command with a particular capability for performing a security function agrees to perform the function for another;

e. A command is established expressly to provide centralized service (e.g., Personnel Support Activity or Human Resources Office); or

f. When either a cleared contractor or a long term visitor group is physically located at a DON command.

2. The SSA shall be specific and shall clearly define the security responsibilities of each participant. The agreement shall include requirements for advising commanding officers of any matter(s) which may directly affect the security integrity of the command.

2-11 INSPECTIONS, ASSIST VISITS, AND PROGRAM REVIEWS

1. Commanding officers are responsible for evaluating the security posture of their subordinate commands.

2. Senior commanders may, as determined necessary, conduct inspections, assist visits, and reviews to examine overall security posture of subordinate commands. Unless otherwise required, it is not necessary to conduct separate inspections for security. They may be conducted during other scheduled inspections and results identified as such (see **exhibit 2C**).

3. Refer to **appendix D** of reference (b) for the PSP inspection checklist.

2-12 FORMS

Appendix B lists the forms used in the ISP along with purchasing information.

2-13 REPORT CONTROL SYMBOLS

Appendix C lists the report control symbols required by this regulation.

REFERENCES

(a) DoD 5220.22-M, *National Industrial Security Program Operating Manual (NISPOM)*, Jan 95 (NOTAL)

(b) SECNAVINST 5510.30A, *DON Personnel Security Program Regulation*, 10 Mar 99

(c) OPNAVINST 3120.32C, *Standard Organization and Regulations of the U.S. Navy*, 11 Apr 94 (NOTAL)

(d) CMS-1A, *Cryptographic Security Policy and Procedures Manual (U)*, 25 Feb 98 (NOTAL)

(e) NWP 1-01, *Naval Warfare Publications Systems*, Nov 94 (NOTAL)

(f) OPNAVINST C5510.101D, *NATO Security Procedures (U)*, 17 Aug 82 (NOTAL)

(g) *Defense Federal Acquisition Regulation, Subpart 201.602-2*

(h) OPNAVINST 5239.1A, *Department of the Navy Automatic Data Processing Security Program*, 3 Aug 82

(i) DoD 5105-21-M-1, *DoD Sensitive Compartmented Information Administrative Manual*, 3 Aug 98 (NOTAL)

(j) Director, Central Intelligence Directive (DCID) 1/14, *Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information (SCI)*, 2 Jul 98 (NOTAL)

(k) OPNAVINST 5530.14C, *DON Physical Security and Loss Prevention*, 10 Dec 98 (NOTAL)

EXHIBIT 2A

GUIDELINES FOR COMMAND SECURITY INSTRUCTION

1. The security manager shall assess the vulnerability of the command classified information to loss or compromise. This includes obtaining information on the local threat, volume and scope of classified information, mission of the command, countermeasures available and the cost, and the effectiveness of alternative courses of action. Results of this assessment shall be used to develop a command security instruction which will emulate the organization of this regulation and identify any unique command requirements. The command security instruction shall supplement this regulation and other directives from authorities in the command administrative and operational chain.

2. Incorporate the following into the command security instruction:

a. The purpose, applicability, and relationship to other directives, particularly this regulation.

b. Identify the chain of command.

c. Describe the security organization and identify positions.

d. Cite and append SSAs, if applicable.

e. Describe procedures for internal and subordinate security reviews and inspections.

f. Specify internal procedures for reporting and investigating loss, compromise, and other security discrepancies.

g. Establish procedures to report CI matters to the nearest NCIS office.

h. Develop an ISP security education program. Assign responsibilities for briefings and debriefings.

i. State whether the commanding officer and any other command officials have been delegated Top Secret or Secret original classification authority.

j. Establish procedures for the review of classified information prepared in the command to ensure correct classification and marking. Identify the sources of security classification guidance commonly used, and where they are located.

k. Develop an industrial security program and identify key personnel, such as the COR, if applicable.

l. Specify command responsibilities and controls on any special types of classified and controlled unclassified information.

m. Establish reproduction controls to include compliance with reproduction limitations and any special controls placed on information by originators.

n. Identify requirements for the safeguarding of classified information to include how classified information shall be protected during working hours; stored when not in use; escorted or handcarried in and out of the command; and protected while in a travel status. Other elements of command security which may be included are key and lock control; safe and door combination changes; location of records of security container combinations; procedures for emergency access to locked security containers; protecting telephone conversations; conducting classified meetings; the safeguarding of U.S. classified information located in foreign countries; AIS processing equipment; and residential storage arrangements.

o. Establish command destruction procedures. Identify destruction facilities or equipment available. Attach a command emergency destruction plan, as a supplement, when required.

p. Establish command visitor control procedures to accommodate visits to the command involving access to, or disclosure of, classified information. Identify procedures to include verification of personnel security clearances and need-to-know.

3. Refer to SECNAVINST 5510.30A for guidance concerning personnel security investigations, adjudications, and clearances.

EXHIBIT 2B

EMERGENCY PLAN AND EMERGENCY DESTRUCTION SUPPLEMENT

PART ONE: EMERGENCY PLAN

1. Commanding officers shall develop an emergency plan for the protection of classified information in case of a natural disaster or civil disturbance. This plan may be prepared in conjunction with the command's disaster preparedness plan.

2. Emergency plans provide for the protection of classified information in a way that will minimize the risk of personal injury or loss of life. For instance, plans should call for immediate personnel evacuation in the case of a fire, and not require that all classified information be properly stored prior to evacuation. A perimeter guard or controlling access to the area will provide sufficient protection without endangering personnel.

3. In developing an emergency plan, assess the command's risk posture. Consider the size and composition of the command; the amount of classified information held; situations which could result in the loss or compromise of classified information; the existing physical security measures; the location of the command and degree of control the commanding officer exercises over security (e.g., a ship versus a leased private building); and local conditions which could erupt into emergency situations.

4. Once a command's risk posture has been assessed, it can be used to develop an emergency plan which can take advantage of a command's security strengths and better compensate for security weaknesses. At a minimum, the emergency plan shall designate persons authorized to decide that an emergency situation exists and to implement emergency plans; determine the most effective use of security personnel and equipment; coordinate with local civilian law enforcement agencies and other nearby military commands for support; consider transferring classified information to more secure storage areas in the command; designate alternative safe storage areas outside the command; identify evacuation routes and destinations; arrange for packaging supplies and moving equipment; educate command personnel in emergency procedures; give security personnel and augmenting forces additional instruction on the emergency plan; establish procedures for prompt notification of appropriate authorities in the chain of command; and establish the requirement to assess the integrity of the classified information

after the emergency (even though a document-by-document inventory may not be possible under current accountability guidelines).

PART TWO: EMERGENCY DESTRUCTION SUPPLEMENT

1. Commands located outside the U.S. and its territories and units that are deployable, require an emergency destruction supplement for their emergency plans (CMS-1A provides additional emergency destruction policy and guidance for commands that handle COMSEC information). Conduct emergency destruction drills as necessary to ensure that personnel are familiar with the plan and associated equipment. Any instances of incidents or emergency destruction of classified information shall be reported to the CNO (N09N2).

2. The priorities for emergency destruction are: Priority One--Top Secret information, Priority Two--Secret information, and Priority Three--Confidential information.

3. For effective emergency destruction planning, limit the amount of classified information held at the command and if possible store less frequently used classified information at a more secure command. Consideration shall be given to the transfer of the information to AIS media, which will reduce the volume needed to be transferred or destroyed. Should emergency destruction be required, any reasonable means of ensuring that classified information cannot be reconstructed is authorized.

4. An emergency destruction supplement shall be practical and consider the volume, level, and sensitivity of the classified information held at the command; the degree of defense the command and readily available supporting forces can provide; and proximity to hostile or potentially hostile countries and environments. More specifically, the emergency destruction supplement shall delineate the procedures, methods (e.g., document shredders or weighted bags), and location of destruction; indicate the location of classified information and priorities for destruction; identify personnel responsible for initiating and conducting destruction; authorize the individuals supervising the destruction to deviate from established plans if warranted; and emphasize the importance of beginning destruction in time to preclude loss or compromise of classified information.

5. Naval surface noncombatant vessels operating in hostile areas without escort shall have appropriate equipment on board prepared for use.

YES NO N/A

EXHIBIT 2C

SECURITY INSPECTION CHECKLIST

INTRODUCTION TO THE ISP

___ ___ ___ 1. Does the command hold the current edition of SECNAVINST 5510.36? (1-1)

2. Is the command in possession of the following classified information references: (1-1)

___ ___ ___ a. COMSEC, CMS-1A/CMS-21?
___ ___ ___ b. DoD SCI Security Manual/relevant DCIDs?
___ ___ ___ c SAPs, OPNAVINST S5460.4C?
___ ___ ___ d. SIOP and SIOP-ESI, OPNAVINST S5511.35K?
___ ___ ___ e. NNPI, NAVSEAINST C5511.32B?
___ ___ ___ f. RD/FRD, DoD Directive 5210.2?
___ ___ ___ g. CNWDI, DoD Directive 5210.2?
___ ___ ___ h. NATO, OPNAVINST C5510.101D?
___ ___ ___ i. Classified information released to industry, NISPOM?
___ ___ ___ j. Controlled unclassified information, DoD 5200.1-R?

___ ___ ___ 3. Are waivers and exceptions submitted to the CNO (N09N2) for all conditions that prevent compliance with SECNAVINST 5510.36? (1-2)

COMMAND SECURITY MANAGEMENT

1. Has the commanding officer: (2-1)

___ ___ ___ a. Issued a command security instruction?
___ ___ ___ b. Approved an emergency plan for the protection and destruction of classified information?
___ ___ ___ c. Established an Industrial Security Program?
___ ___ ___ d. Ensured that the security manager and other personnel have received security education and training?
___ ___ ___ e. Ensured that personnel are evaluated on the handling, creation or management of classified information on performance evaluations?

YES NO N/A

2. To implement the ISP, has the commanding officer designated in writing a command?

___ ___ ___ a. Security manager? (2-2)
___ ___ ___ b. TSCO? (2-3)
___ ___ ___ c. TSCA? (2-3)
___ ___ ___ d. Assistant security manager? (2-4)
___ ___ ___ e. Security assistant(s)? (2-4)
___ ___ ___ f. CMS custodian and alternate? (2-5)
___ ___ ___ g. NWP custodian? (2-5)
___ ___ ___ h. NATO control officer and alternate? (2-5)
___ ___ ___ i. One or more CORs? (2-6)

___ ___ ___ 3. Is the command security manager named and identified to command personnel on command organizational charts, telephone listings, rosters, or other media? (2-2)

4. Has the command security manager: (2-2)

___ ___ ___ a. Developed a command security instruction?
___ ___ ___ b. Formulated, coordinated, and conducted a command security education program?
___ ___ ___ c. Kept command personnel abreast of all changes in security policies and procedures?
___ ___ ___ d. Reported and investigated all security threats and compromises?
___ ___ ___ e. Promptly referred all incidents, under their jurisdiction, to the NCIS?
___ ___ ___ f. Coordinated the preparation of the command SCGs?
___ ___ ___ g. Maintained liaison with the PAO on proposed media releases?
___ ___ ___ h. Developed security procedures for visitors who require access to classified information?
___ ___ ___ i. Implemented regulations concerning the disclosure of classified information to foreign nationals?

___ ___ ___ 5. Does the TSCO manage and control all command TS information, less SCI? (2-3)

YES	NO	N/A	
—	—	—	6. Are security functions performed by another command covered by a written SSA? (2-10)
—	—	—	7. Have qualified security inspectors conducted command inspections, assist visits, and program reviews to examine the command's overall security posture? (2-11)

SECURITY EDUCATION

—	—	—	1. Does the command have an effective information security education program? (3-1)
			2. Is additional ISP training provided to? (3-3)
—	—	—	a. Approved OCAs?
—	—	—	b. Derivative classifiers, security managers, and other security personnel?
—	—	—	c. Classified couriers?
—	—	—	d. Declassification authorities?

CLASSIFICATION MANAGEMENT

—	—	—	1. Is information classified only to protect NSI? (4-1)
—	—	—	2. Do procedures prohibit the use of terms such as "For Official Use Only" or "Secret Sensitive" for the identification of classified information? (4-2)
—	—	—	3. Have the command OCAs been trained in their duties and responsibilities? (4-6)
—	—	—	4. Has written confirmation of this training (i.e., indoctrination letter) been submitted to the CNO (N09N2)? (4-6)
—	—	—	5. Is information, not officially released or disclosed to the public, classified or reclassified only if the information meets the criteria of E.O. 12958? (4-11)
—	—	—	6. Is the classification level, of any information believed to be improperly classified, challenged? (4-12)

YES NO N/A

___ ___ ___ 7. Does NATO and FGI retain its original classification level and is it assigned an English classification equivalent, if necessary? (4-17, 6-14)

___ ___ ___ 8. Are procedures established for the completion of command mandatory declassification reviews within 45 working days? (4-23)

___ ___ ___ 9. Are reasonable steps taken to declassify information determined to be of permanent historical value prior to their accession into NARA? (4-25)

___ ___ ___ 10. Have cognizant OCAs notified holders of unscheduled classification changes involving their information? (4-26)

SECURITY CLASSIFICATION GUIDES

___ ___ ___ 1. Is a SCG issued for each classified system, program, plan, or project before the initial funding or implementation of the system, program, plan, or project? (5-1)

___ ___ ___ 2. Is each SCG approved personally and in writing by an OCA who has program or supervisory responsibility over the information? (5-2)

___ ___ ___ 3. Are command SCGs formatted per OPNAVINST 5513.1E? (5-2)

___ ___ ___ 4. Are command-originated SCGs reviewed, by the cognizant OCA, at least every 5 years? (5-4)

___ ___ ___ 5. Are all changes promptly submitted to the Rankin Program Manager? (5-4)

MARKING

___ ___ ___ 1. Are classified documents and their portions properly marked to include all applicable basic and associated markings? (6-1, 6-5)

YES	NO	N/A		
—	—	—	2.	Are originally classified documents marked with a "Classified by" and "Reason" line? (6-8)
—	—	—	3.	Are derivatively classified documents marked with a "Derived from" line? (6-9)
—	—	—	4.	Is "Multiple Sources" annotated on the "Derived from" line of classified documents derived from more than one source? (6-9)
—	—	—	5.	Is a source listing attached to the file copy of all documents classified by "Multiple Sources?" (6-9)
—	—	—	6.	Are downgrading and declassification instructions included on all classified documents, less exception documents? (6-10)
—	—	—	7.	Are the appropriate warning notices placed on the face of classified documents? (6-11)
—	—	—	8.	Are classified intelligence documents/portions marked with the appropriate intelligence control marking(s)? (6-12)
—	—	—	9.	Are the portions of documents containing NATO and FGI marked to indicate their country of origin? (6-14)
—	—	—	10.	Is the face of NATO and foreign government RESTRICTED documents and FGI marked with the appropriate notice? (6-15)
—	—	—	11.	Is the assignment and use of nicknames, exercise terms, and code words per OPNAVINST 5511.37C? (6-17)
—	—	—	12.	Is an explanatory statement included on the face of documents classified by compilation? (6-18)

YES NO N/A

___ ___ ___ 13. Do documents, marked classified for training and test purposes, include a statement indicating that the documents are actually unclassified? (6-20)

___ ___ ___ 14. When removed or used separately, are component parts of classified documents marked as separate documents? (6-21)

___ ___ ___ 15. Are letters of transmittal marked to show the highest overall classification level of any information being attached or enclosed? (6-24)

___ ___ ___ 16. Are electronically transmitted messages properly marked? (6-25)

___ ___ ___ 17. Are classified files or folders marked or have the appropriate SFs been attached to indicate the highest overall classification level of the information contained therein? (6-26)

___ ___ ___ 18. Are all classified materials such as AIS media, maps, charts, graphs, photographs, slides, recordings, and videotapes appropriately marked? (6-27 through 6-34)

SAFEGUARDING

___ ___ ___ 1. Does the command ensure that all DON employees (military and civilian) who resign, retire, separate, or are released from active duty, return all classified information in their possession? (7-1)

___ ___ ___ 2. Is TS information including copies, originated or received by the command, continuously accounted for, individually serialized, and entered into the command's TS inventory? (7-3)

___ ___ ___ 3. Are command TS documents and material physically sighted at least annually? (7-3)

___ ___ ___ 4. Does the command have control measures in place for the receipt and dispatch of Secret information? (7-4)

YES	NO	N/A	
—	—	—	5. Are control measures in place to protect unauthorized access to command TS, Secret, or Confidential information? (7-3, 7-4, 7-5)
			6. Are working papers: (7-6)
—	—	—	a. Dated when created?
—	—	—	b. Marked "Working Paper" on the first page?
—	—	—	c. Marked with the highest overall classification, center top and bottom, of each applicable page?
—	—	—	d. Destroyed when no longer needed?
—	—	—	e. Brought under accountability after 180 days or when they are released outside the command?
—	—	—	7. Are appropriate control measures taken for other special types of classified information? (7-7)
—	—	—	8. Are SFs 703, 704, and 705 placed on all classified information when removed from secure storage? (7-9)
—	—	—	a. Are SFs 706, 707, 708, and 712 being utilized on all classified AIS media?
—	—	—	b. Are classified typewriter ribbons, carbon sheets, plates, stencils, drafts, and notes controlled, handled, and stored per their classification level?
—	—	—	9. Has the command established procedures for end of day security checks, to include the use of SFs 701 and 702? (7-10)
—	—	—	10. Are classified vaults, secure rooms, and containers made an integral part of the end of day security check? (7-10)
—	—	—	11. Are procedures in place to ensure that visitors have access only to information for which they have a need-to-know and the appropriate clearance level? (7-11)

YES NO N/A

___ ___ ___ 12. Are procedures in place for classified meetings held at the command or hosted at cleared facilities? (7-12)

___ ___ ___ 13. Is classified information reproduced only to the extent that is mission essential? (7-13)

DISSEMINATION

___ ___ ___ 1. Are procedures established to ensure the proper dissemination of classified information outside DoD and to foreign governments? (8-1)

___ ___ ___ 2. Are special types of classified and controlled unclassified information disseminated per their governing instructions? (8-4)

___ ___ ___ 3. Is information disseminated to Congress per SECNAVINST 5730.5 and OPNAVINST 5510.158? (8-6)

___ ___ ___ 4. Do all newly generated classified and unclassified technical documents include a distribution statement listed in **exhibit 8A** of SECNAVINST 5510.36? (8-7)

___ ___ ___ 5. Are all DoD-funded RDT&E programs that involve Navy scientific and technical information and unclassified technical data that reveal critical technology disseminated per their applicable instruction? (8-7)

___ ___ ___ 6. Is command information intended for public release, including information released through AIS means (i.e., INTERNET, computer servers), submitted for prepublication review? (8-8)

TRANSMISSION AND TRANSPORTATION

___ ___ ___ 1. Is classified information transmitted and transported only per specific requirements? (9-2, 9-3, 9-4)

YES NO N/A
17 MAR 1999

2. Are special types of classified information transmitted and transported per their governing instructions? (9-5)

3. Are command personnel advised not to discuss classified information over unsecured circuits? (9-6)

4. Are command procedures established for preparing classified bulky shipments as freight? (9-7)

5. Is classified information transported or transmitted outside the command receipted for? (9-10)

6. Does the command authorize the handcarry or escort of classified information, via commercial aircraft, only if other means are not available, and there is an operational need or contractual requirement? (9-11)

7. Are designated couriers briefed on their courier responsibilities and requirements? (9-11)

8. Are procedures established for the control and issuance of the DD 2501? (9-12)

STORAGE AND DESTRUCTION

1. Are any command weaknesses, deficiencies, or vulnerabilities in any equipment used to safeguard classified information reported to the CNO (N09N3)? (10-1)

   a. Does the command ensure that weapons, money, jewelry or narcotics are not stored in security containers used to store classified information?

   b. Does the command ensure that external markings on command security containers do not reveal the level of information stored therein?

YES NO N/A

2. Does command security equipment meet the minimum standards of GSA? (10-2)

3. Does the command meet the requirements for the storage of classified bulky information? (10-3)

4. Does the command mailroom have a GSA-approved security container to store USPS first class, certified, and registered mail overnight? (10-3)

5. Are command vaults and secure rooms, not under visual control at all times during duty hours, equipped with electric, mechanical, or electro-mechanical access control devices? (10-7)

6. Are specialized security containers securely fastened to the structure, rendering them non-portable? (10-8)

7. Has the command removed all containers manufactured by Remington Rand? (10-9)

8. Is classified information removed from designated work areas for work at home done so only with prior approval of appropriate officials? (10-10)

9. Are command container combinations changed: (10-12)

   a. By individuals who possess the appropriate clearance level?
   b. Whenever the container is first put into use?
   c. Whenever an individual knowing the combination no longer requires access to the container (unless other sufficient controls exist to prevent access)?
   d. Whenever a combination has been subjected to compromise?
   e. Whenever the container is taken out of service?

YES	NO	N/A		
__	__	__	10.	Are command container combinations marked, and accounted for per the classification level of the information stored therein? (10-12)
__	__	__	11.	Is there an SF 700 affixed inside each command security container? (10-12)
__	__	__	12.	Does the SF 700 include the names, home addresses, and phone numbers of all persons having knowledge of the combination? (10-12)
__	__	__	13.	Has the command established procedures for command key and padlock accountability and control? (10-13)
__	__	__	14.	Are command locks repaired only by authorized personnel who have been subject to a trustworthiness determination or who are continuously escorted? (10-15)
__	__	__	15.	Are command security containers, previously placed out of service, marked as such on the outside and the "Test Certification Label" removed on the inside? (10-15)
__	__	__	16.	Are command security containers, with visible repair results, marked as such with a label posted inside the container stating the details of the repairs? (10-15)
__	__	__	17.	Are all commercial IDSs used on command security containers, vaults, modular vaults, and secure rooms approved by the CNO (N09N3)? (10-16)
__	__	__	18.	Is command classified information destroyed when no longer required? (10-17)
__	__	__	19.	Do all command shredders, pulverizers, and disintegrators meet the minimum requirements? (10-18)
__	__	__	20.	Has the command established effective procedures for the destruction of classified information? (10-19)

YES NO N/A

21. When filled, are command burn bags sealed and safeguarded per the highest overall classification level of their contents? (10-19)

22. Is controlled unclassified information destroyed per the governing instructions? (10-20)

INDUSTRIAL SECURITY PROGRAM

1. Has the command established an Industrial Security Program? (11-1)

2. Has the command developed a PPP? (11-1)

3. Has the commanding officer established or coordinated oversight over classified work carried out by cleared DoD contractor employees in spaces controlled or occupied at DON shore commands? (11-5)

4. Have all FADs been issued per SECNAVINST 5510.30A? (11-6)

5. Does the command COR: (11-8)

   a. Complete, issue, and sign all DD 254s?
   b. Validate all contractor security clearances?
   c. Verify FCLs and storage capability prior to release of classified information?
   d. Certify and approve all DD 1540s?
   e. Provide additional security requirements?
   f. Review all reports of industry security violations and forward to program managers?
   g. Coordinate DD 254 reviews and guidance, as needed?
   h. Verify that cleared DoD contractor employees who are used as couriers have been briefed on their courier responsibilities? (11-12)

YES	NO	N/A	
—	—	—	6. Is classified intelligence information disclosed only to those contractors cleared under the NISP? (11-14)

LOSS OR COMPROMISE OF CLASSIFIED INFORMATION

—	—	—	1. Since the last inspection, has the command had any incidents involving a loss or compromise of classified information? (12-1)
—	—	—	2. If a possible loss or compromise occurred, was a PI conducted? (12-4)
—	—	—	3. If a significant command weakness is identified, or a confirmed loss or compromise occurred, was a JAGMAN investigation conducted? (12-9)
—	—	—	4. When a loss or compromise of classified information or equipment has occurred, is appropriate investigative and remedial action(s) taken to ensure further loss or compromise does not recur? (12-14)
—	—	—	5. Is appropriate and prompt corrective action taken whenever a knowing, willful, or negligent compromise or repeated administrative disregard of security regulations occurs? (12-14)
—	—	—	6. Are procedures established for review of investigations by seniors? (12-14)
—	—	—	7. Are security reviews conducted on information subjected to loss or compromise? (12-15)
—	—	—	8. Are procedures established for classification reviews by originators or OCAs? (12-16)
—	—	—	9. Is receipt of improperly transmitted information reported to the sender? (12-19)